Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

WRITTEN *EX PARTE* SUBMISSION OF HUAWEI TECHNOLOGIES CO., LTD AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit this *ex parte* presentation to supplement the record in the above-captioned docket.

Some comments in this proceeding have questioned whether a testing and certification regime would be sufficient to guard against potential threats to national security from particular manufacturers. Huawei has been one of the most advanced practitioners in the telecom industry when it comes to cybersecurity testing and certification. In addition to Common Criteria and other standard security review processes, the United Kingdom, a close ally of this Nation, has worked with Huawei to adopt a cybersecurity review process for Huawei equipment. In consultation with the UK government, Huawei has established a "Huawei Cyber Security Evaluation Centre" (HCSEC) in the UK, which is monitored by a public–private Oversight Board to ensure its independency and efficacy. The HCSEC is financed by Huawei, and staffed by around 40 individuals with UK security clearances who evaluate the security of a range of products deployed in the UK

telecommunications market that may have national security implications. A board primarily composed of British intelligence officers and government officials oversees all of the work at the testing center:

> The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the [the UK Government's National Cyber Security Centre (NCSC)], and an executive member of [the Government Communications Headquarters (GCHQ)]'s Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector.[1]

The HCSEC Oversight Board aims "to continue to provide assurance to the UK Government by ensuring openness, transparency and responsiveness to Government and UK customer security concerns" through the cybersecurity-oriented cooperation mechanism among Huawei, the UK Government and UK network operators.[2] The Oversight Board releases annual reports of its findings. This year's report is the fourth.

Each year's Oversight Board report has concluded that HCSEC provides high quality technical assessments and cyber security expertise.[3] Further, the Oversight Board has concluded that

---

[1] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, 2018 Annual Report (2018 Report) at 7, available at https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018. The Board's earlier reports are available at https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2015 (2015 Report); https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2016 (2016 Report); and https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2017 (2017 Report).

[2] 2018 Report at 9.

[3] 2015 Report at 3 ("the technical assessments conducted have been of consistently high quality and have provided useful risk management information to both the Government and the

"rigorous" annual audits by an outside party provide assurance that HCSEC operates independently of undue influence from elsewhere in Huawei.[4]

As a whole, the 2018 Oversight Board report positively affirms the mechanisms and models for cybersecurity collaboration that Huawei, the UK government, and UK operators have adopted. The report concludes that, "In the year 2017-18, HCSEC fulfilled its obligations in respect of the technical work required of it by NCSC. The capability of HCSEC has improved in 2017. It is evident that HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK."[5] As indicated in the report, Huawei has demonstrated openness, transparency and responsiveness in its approach to cyber security. "It is to be welcomed that despite difficulties, Huawei has continued to work closely with NCSC and HCSEC and provided access and information when requested."[6]

The 2018 Report also notes that the Board had some concerns with certain Huawei engineering processes. The 2018 Report states that plans have been developed to address these concerns and that remediation work is underway.[7] Some press reports have focused on the Board's

---

[communication service providers]"); 2016 Report at 3-4 ("HCSEC's cybersecurity capability has continued to improve" and it is a "competent and effective organization"); 2017 Report at 4 ("HCSEC continues to provide unique, world-class cyber security expertise and technical assurance"); 2018 Report at 3 ("HCSEC continues to provide unique, world-class cyber security expertise and technical assurance").

4 2015 Report at 3; 2016 Report at 4; 2017 Report at 4; 2018 Report at 3.

5 2018 Report at 25.

6 2018 Report at 12.

7 2018 Report at 13 (para. 3.5); 15 (paras. 3.15, 3.17); 16 (paras. 3.21-3.22).

stated concerns, without discussing the context of remediation efforts that are underway. The 2018 Report, however, does not suggest or even imply that a technical review and oversight process is ineffective. To the contrary, it states that the NCSC "still believes that the assurance model including HCSEC is the best way to manage the risk of Huawei's involvement in the UK telecommunications sector." [8] Indeed, the fact that the 2018 Report identified these technical issues demonstrates that the oversight process is effective in detecting and averting potential problems. Huawei is grateful for this feedback and is developing the necessary risk management and mitigation mechanism to drive active improvement.

Finally, it is worthwhile to note that the HCSEC, like other security certification bodies, has never found any malicious code or backdoor in Huawei's products.

[8] 2018 Report at 18.

Respectfully submitted,
___/s/_____

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson

JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons
Catherine Kuersten

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com
catherine.kuersten@morganlewis.com

Counsel to Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.